FREEDIAMETER
PRESENTATION & TUTORIAL

Souheil Ben Ayed (Keio), Sebastien Decugis (NICT) WIDE AAA working group
A short introduction to Diameter

~ 15 minutes
Diameter: AAA protocol

- Diameter:
  - Transports AAA data
  - Designed for network access control.
  - Extensible and extended

- RADIUS evolution
- 10 years maturity (?)
Diameter message format

- **Message header:**
  - Application Id
    - App 0: Diameter Base Proto
  - Command-Code & Flags
    - Ex: Accounting-Request, ...
- **Any number of AVP(s)**
  - Code, flags
  - Data (integers, strings, ...)
- **Dictionary for AVP**
Diameter: dual scope

- One message format, two scopes:
  - Diameter network management ("Diameter link layer")
  - AAA applications data ("Diameter application layer")

- At link layer, Diameter is a peer-to-peer protocol
  - All nodes are equivalent, forming an overlay network.

- At application layer, we have roles:
  - Clients, agents (ex: proxies), servers.
Diameter properties

- **Lower layers:**
  - Reliable (TCP, SCTP)
  - Secure (IPsec, TLS)
    - Hop-by-hop model
    - Mutual authentication

- **Failover, retransmissions**

- **Traceability**

- **Routing**
  - App. & realm based.
Diameter link management

- Defined in Diameter Base Protocol (RFC3588):
  - Messages:
    - Application Id : 0
    - Capabilities-Exchange
    - Device-Watchdog
    - Disconnect-Peer
  - Peers State Machines
    - Not so complex when you separate initiator and receiver states
Routing:

- Some AVP are used for routing:
  - Destination-Realm, [Destination-Host]
    - May derive from the user NAI (user@realm.net) in User-Name
  - The application id (in header) is also used.
    - Ex: allows EAP messages to reach an EAP server in realm.net
    - Nodes don’t need a view of the global network
      - The servers may dynamically be discovered from DNS (NAPTR)
  - Routing of answers is very simple, always reverse path.
    - Mechanism based on end-to-end and hop-by-hop ids.

Traceability:

- Each node adds a Route-Record AVP when forwarding.
Reliable lower layer is not sufficient for reliability
- Ex: software can crash on a relay during forwarding.

Mechanism of failover:
- All requests are kept until answer is received
- If the link goes down, the request is re-sent through another link, or an error is generated.
Diameter Sessions

- Sessions
  - Correlates messages that are related to the same service and end-user, using Session-Id AVP. Example:
    - Several DER/DEA messages for authentication, authorization
    - Periodical ACR/ACA while the user uses the network
    - STR/STA at the end of service provision.

- The Base Protocol provides the framework to support these sessions: Session State Machine, commands, AVPs (ex: Auth-Session-State, ASR/ASA, …)
Diameter Extensibility

- Extensibility of the protocol:
  - By definition of new AVPs, Commands, and/or Applications.
  - Vendors-defined AVPs supported.
  - Many applications are already defined
    - Ex: Diameter SIP, Credit Control, PMIP6, ...

- Diameter Base Protocol is specified in RFC3588
  - Revised soon (?) in RFC3588bis
    - Simplified state machine, better TLS handling, ...

Souheil Ben Ayed, Sebastien Decugis
Any question so far?

Souheil Ben Ayed, Sebastien Decugis